

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

In the Matter of)	
)	
Advanced Methods to Target and Eliminate)	CG Docket No. 17-59
Unlawful Robocalls)	
)	
Call Authentication Trust Anchor)	WC Docket No. 17-97

COMMENTS OF ZipDX LLC

**5th/4th FURTHER NOTICES OF PROPOSED RULEMAKING
Re: Gateway Providers & Foreign-Originated Calls**

Our serious battle against illegal robocalls has been on-going for more than a decade. Yet from an American consumer's perspective, there appears to have been little progress. The barrage of calls continues unabated.

The instant FNPRM potentially reflects an important shift in regulatory and enforcement focus, away from sweeping efforts to engage the entire universe of telecom providers, consisting of thousands of entities, toward a focus on the small subset of that universe that is at the root of the problem. There is a set of providers, both foreign and domestic, that insist on accepting money to put illegal calls onto the network. That set of providers needs to be forced to give up the revenue associated with this traffic. Those providers that depend on illegal robocalls for all or most of their income must find another line of business or close up shop.

We believe the best approach is to use rules and enforcement efforts to engage the most relevant providers as part of the solution. Simple rules are best; we already have several. Distinguishing providers among foreign and domestic, or originating and gateway and intermediate, is problematic; focus instead on those providers that are closest to the call source and are motivated to follow the rules. Guide providers to segregate and scrutinize high-volume traffic, which is, by definition, where illegal robocalls flow.

We open our comments with some real-world observations about how the call-laundering ecosystem functions. Next, we address specific issues raised in the FNPRM. Guided by the FNPRM discussion, in our conclusion we put forth a framework that will be simple and effective in addressing this scourge. The most important distinction we can make is between conversational and non-conversational (high-volume) traffic flows. Those that elect to handle non-conversational traffic, which is where illegal robocalls hide in plain sight, will bear the burden of keeping them off our network.

TABLE OF CONTENTS

ILLEGAL ROBOCALLING BACKGROUND	4
Intermediate vs. Originating Providers	4
Foreign vs. Domestic Providers	5
Financial Analysis of Illegal Robocalling	6
Limitations of STIR/SHAKEN	9
 FNPRM SPECIFIC RESPONSES	 10
Need for Action	10
Scope of Requirements and Definitions	13
Authentication	18
Robocall Mitigation	19
Robocall Mitigation Database	32
Alternative Approaches	34
Expected Benefits and Costs	36
 SUMMARY AND CONCLUSIONS	 37

ILLEGAL ROBOCALLING BACKGROUND

A. Intermediate vs. Originating Providers

Current and proposed regulations draw significant distinctions between originating and intermediate providers, placing different obligations on each.¹ This is quite problematic. As has been previously noted, the role that a provider plays can vary on a call-by-call basis.² What is worse is that often providers do not themselves know in what role they are serving.

The Comments of Belgacom International Carrier Services SA (BICS)³, already filed in this docket, are an illuminating example. BICS explains:

- “The nature of such traffic is not always clear and obvious to gateway and intermediate providers as they are not the traffic originators.” (page 1)
- “[Gateway and intermediate providers] have no details on the traffic origination” (page 1)
- “[T]he nature of the traffic ... is not always known to the gateway and intermediate providers” (page 1)
- “Gateway providers are not aware of the traffic origination nor the nature of the traffic.” (page 1)
- “[W]e cannot guarantee though that BICS sending parties will also collaborate with Traceback requests as they will be obliged by their local legislations, regulations and contractual provisions.” (page 2)
- “[G]ateway providers are unable, in most cases, to determine the origin and nature of each and every calls (as explained above).” (page 2)
- “[Gateway providers] do not know the origin of the calls and that they do not know the nature of the traffic.” (page 3)

This is at the crux of our problem. BICS’ comments are not extraordinary; they align with what we know from speaking with numerous gateway, intermediate and foreign providers involved in illegal robocalling. They often know very little about their customers and their customers’ traffic.

¹ See Footnote 20 of the FNPRM, noting that the Commission uses the term “Voice Service Provider” differently in different regulations and contexts; it always includes Originating and Terminating providers, but sometimes it also includes Intermediate Providers and sometimes it does not.

² See Paragraph 17 of the FNPRM.

³ Comments from Belgacom International Carrier Services SA on the draft Fifth Further Notice of Proposed Rulemaking and Fourth Further Notice of Proposed Rulemaking, dated 2021-11-18 and ECFS filed 2021-11-22. <https://ecfsapi.fcc.gov/file/112209653493/BICS%20comments.pdf>

With this lack of knowledge, they cannot know if their customer is operating as an originator, an intermediate provider, or an end-user for any given call, and thus they cannot know what role they are serving as the next provider in line. They only know that they are getting paid to funnel traffic into the USA telephone network and profiting from that activity. It should come as no surprise that with this level of disregard for the sanctity of our network, we face a never-ending barrage of unwanted calls.

We found 253 providers in the Robocall Mitigation Database that have two entries: one as an intermediate provider, and the other not (based on both providers using the same FRN), BICS being one of them. Absent some explicit prior arrangement, a downstream provider accepting traffic from a provider in this group of 253 would not know if the source were acting as an intermediate provider or an originating provider, or even as an end-user, for any given call.

B. Foreign vs. Domestic Providers

Given the recognition that many illegal robocalls are foreign-sourced, distinguishing between domestic and foreign providers could be helpful. But it is not always straightforward. BICS is listed in the 499A filer database⁴ as headquartered in Belgium. But the RMD entry for BICS as an Intermediate Provider curiously shows United States of America as the Country for Business Address and the Contact Country.⁵ The other BICS RMD entry shows Belgium in both fields.⁶

⁴ <https://apps.fcc.gov/cgb/form499/499detail.cfm?FilerNum=826394>

⁵

https://fccprod.servicenowservices.com/rmd?id=rmd_form&table=x_g_fmc_rmd_robocall_mitigation_database&sys_id=809eb7a21befa01002beea82f54bcbea&view=sp

⁶

https://fccprod.servicenowservices.com/rmd?id=rmd_form&table=x_g_fmc_rmd_robocall_mitigation_database&sys_id=4eca45b21b683050e4ec848ce54bcbc2&view=sp

The Commission's Enforcement Bureau recently sent Cease and Desist letters to several providers.⁷ The letter to PZ/Illum is addressed to CEO Prince Anand with a California address.⁸ But PZ Telecommunication LLC's 499A entry, while showing the same California address for the business, indicates the CEO's address is "B-12 P & T SOCIETY NEAR VEJALPUR RAILWAY STATION O AHMEDABAD GUJARAT 380051" – in INDIA.⁹

The C&D letter to Primo Dialler went to CEO Mohammed Mashadi in Wyoming.¹⁰ But his LinkedIn Profile says he is based in West Midlands, England.¹¹ Primo Dialler is in the RMD database twice; once as an intermediate provider and once not.

The Indiana Attorney General has filed suit against a provider called Startel.¹² In its complaint, the Indiana AG indicates that StarTel's CEO is in India and that the company has numerous ties to India, despite claiming an Indiana address. (The difference between India and Indiana is "NA" – go figure.)

Clearly it is challenging to know if BICS, PZ Telecommunication, Primo Dialler, Startel, and a host of others are foreign or domestic.

C. Financial Analysis of Illegal Robocalling

Economic analysis can guide how we assess the impact of certain regulations, a technique routinely used by the Commission. Many have expressed concern about new constraints that

⁷ <https://www.fcc.gov/document/fcc-issues-robocall-cease-and-desist-letters-3-more-companies>

⁸ <https://docs.fcc.gov/public/attachments/DOC-376749A1.pdf>

⁹ <https://apps.fcc.gov/cgb/form499/499detail.cfm?FilerNum=833823>

¹⁰ <https://docs.fcc.gov/public/attachments/DOC-376748A1.pdf>

¹¹ <https://www.linkedin.com/in/mohammed-mashadi-4303087/?originalSubdomain=uk>

¹² State of Indiana v. Startel Communication LLC, et al, United States District Court, Southern District of Indiana, Case 3:21-cv-00150-RLY-MPB, filed 10/14/21.

could impact some Americans roaming abroad.¹³ Concerns have centered on calls originated via foreign mobile networks that use Least Cost Routing to get calls back to the United States.

Assume 40 million Americans travel overseas annually, with each attempting to make 10 calls during their trip; likely high as an average given that received calls are unaffected, as are calls over WiFi and VoLTE and those using over-the-top apps like Skype and Facetime. Suppose 10% of those telco calls are impacted by contemplated regulations, and those callers have to send a text message to the intended call recipient asking that they initiate the call from the USA end. Impute a cost of \$5 to that inconvenience and we get an economic impact of $40 \text{ M} \times 10 \times 0.1 \times \$5 = \$200 \text{ million}$. That number would drop quickly as providers fixed their call routing.

The regulations contemplated are intended to reduce the number of illegal robocalls originating abroad. The Commission has previously estimated economic benefit FLOOR of \$3 billion attributable to wasted time and nuisances if ALL 30 billion annual scam calls were eliminated.¹⁴ Subsequently, the Commission estimated an additional \$10.5 billion in fraud losses annually.¹⁵ If these regulations eliminated just one third of those calls, the benefit would be \$4.5 billion, for a benefit/cost ratio of more than twenty to one. See FNPRM paragraph 108.

We invite commenters to refine our assumptions; the wireless providers have data on how many of their subscribers are roaming, how many calls they initiate back to USA, and how many are doing so over networks that might be impacted by new rules. We cannot find support for a conclusion that the public interest is served by delaying this new rule.

¹³ See the extensive comments filed in WC 17-97 regarding Petitions for Reconsideration of the Second Report and Order; <https://ecfsapi.fcc.gov/file/0114781116291/DA-21-62A1.pdf>.

¹⁴ See the Declaratory Ruling and Third Further Notice of Proposed Rulemaking at paragraph 40 and footnote 87. <https://docs.fcc.gov/public/attachments/FCC-19-51A1.pdf>

¹⁵ See the March 31, 2020 Report and Order and Further Notice of Proposed Rulemaking at paragraph 48. <https://docs.fcc.gov/public/attachments/FCC-20-42A1.pdf> Also FNPRM, para. 4.

It is also instructive to look at the revenue providers derive directly from illegal robocalls. Robocallers pay roughly \$0.001 (one-tenth of a cent) per call to the originating provider that puts their call on the network. That revenue trickles downstream as each call is passed from one provider to the next; each provider absorbs a share as profit.

If there are 30 billion “scam calls” annually (almost all of very short duration), that’s origination revenue of \$30 million, which turns into \$75 million in aggregate revenue across an average of 5 providers in the call chain (originator, three intermediates, and the terminating provider). This is the amount that the industry needs to forego as illegal robocalling is eliminated. It is a trivial amount in the grand scheme of things. (With average revenue per wireless subscriber of \$50, and 300 million US subscribers, the US mobile industry brings in about \$180 BILLION annually.) But to the cottage industry that specializes in this traffic, and to the individuals that earn their living off of it (as company principals and/or commissioned salespeople), it is significant. They will work tooth and nail to hang on to that revenue. They do not care that they are inflicting pain on Americans, measured in economic terms, which is one to two HUNDRED times greater than their own take.

Americans are rightfully extremely resentful of these robocall intrusions – even some “legitimate” robocalls. While television ads interrupt our football games, and web pop-ups interfere with our social media feeds, most people understand that advertising revenue helps to support the content and the delivery platforms that we enjoy. Robocalls, on the other hand, are more urgent and more intrusive, but are delivered via a subscription (landline or wireless) service we pay for, and we get ZERO benefit from that fraction of a penny paid by the robocaller.

D. Limitations of STIR/SHAKEN

The Commission and others have worked tirelessly to define and deploy a Call Authentication Framework. Yet even proponents acknowledge that this is not a panacea nor even a specific limitation on illegal robocalling. It is no more than what the name says: a technology that allows a call recipient to know something about the caller-ID of an incoming call (even if that “something” is nothing).

Five months have passed since the 30-June 2021 deadline for service providers to implement STIR/SHAKEN and certify to it. We found just over 400 “authorized providers” listed by the Policy Administrator as having obtained SHAKEN certificates, required to authenticate calls under the framework.¹⁶ Examining the Robocall Mitigation Database, we found about 2,400 different entities claiming either complete or partial STIR/SHAKEN implementation – a tremendous disparity apparently implicating roughly 2,000 providers.¹⁷

BICS has certified in the RMD under penalty of perjury that it has a partial STIR/SHAKEN implementation, and yet it does not appear on the Policy Administrator’s list of authorized providers. The same for Duratel. PZ Telecommunication claims a COMPLETE implementation and yet has no certificate. Primo Dialler admits they have not implemented STIR/SHAKEN and have filed a woefully inadequate Robocall Mitigation Program.¹⁸

Even if STIR/SHAKEN worked as intended, and notwithstanding the huge number of calls that cannot yet be authenticated because they transit non-IP (legacy) networks, we are faced

¹⁶ See <https://authenticate.iconectiv.com/authorized-service-providers-authenticate>.

¹⁷ We attempted to consolidate affiliated providers by correlating their RMD contact email addresses.

¹⁸ See https://fccprod.servicenowservices.com/api/x_g_fmc_rmd/rmd/attachment?sys=956000241b98b410544a404fe54bcb03

with rampant abuse of telephone numbers. Rogue callers acquire thousands – or even tens of thousands – of telephone numbers so that they can place calls with A-level attestation. This makes their scam calls appear authentic, which is the exact opposite of the framework’s objective. The underlying cost of telephone numbers is zero, encouraging the fraudsters to go down this path.

If the gaming and abuse of STIR/SHAKEN is allowed to continue, this grand framework will end up doing more harm than good.

With this background in mind, we will respond to the specific queries in the FNPRM.

FNPRM SPECIFIC RESPONSES

For each paragraph in the FNPRM which solicits input, and to which we have elected to respond, we show the FNPRM context and question in italics, followed by our comments.

A. Need for Action

25. Are our current rules addressing foreign-originated robocalls sufficient? Existing rules would go a long way in addressing the problem if they were aggressively enforced. Illegal robocallers are, by their nature, rule-breakers. *Rather than adopt new rules, should we leverage our existing rules in new ways to stop such calls?* Enforcement is the best way to increase compliance. *Or should we adopt new rules that rely on methods other than caller ID authentication and robocall mitigation?* If call authentication is not leveraged beyond a checkmark on the call recipient’s phone, it will have missed the mark. *If so, what type of rules should we adopt?* Making providers in the call path responsible for mitigation is the right approach. ALL providers in the path must play a role and be held accountable. Most efficient is

stopping calls at the source, but to the extent that is not effective, enforcement efforts must move rapidly downstream, supported by appropriate underlying rules.

29. *We seek comment on whether these cases [against gateway providers accepting fraud calls from abroad] are representative of the role that some gateway providers play in allowing illegal robocalls to reach U.S. subscribers.* Yes, that conclusion is supported by the evidence I have seen.

30. *We seek comment on the relationship between gateway providers and illegal robocalls entering the U.S. market. Is the problem driven by a few unscrupulous gateway providers that have entered into business arrangements to transit illegal foreign-originated robocall traffic?* Yes. “Few” is likely on the order of several dozen. *Or is the problem more widespread, for instance because gateway providers do not or cannot easily identify bad actors sending illegal robocalls to the United States through the gateway provider’s network?* The providers accepting this traffic elect not to scrutinize their customers or the traffic. It CAN be easily identified by examining a few readily-obtained metrics. *If the problem is widespread, why do gateway providers today decline to identify and act to restrict bad actors and unlawful robocalls?* Those that are accepting this traffic (whether we characterize it as “widespread” or not) fail to identify and restrict it because they get PAID to carry it. They do not want to give up that revenue, and do not want to expend any extra expense or resources just so they can reduce their revenue and profit. *Do foreign originators send illegal robocall traffic to the gateway indirectly, through one or more foreign intermediate providers, in order to conceal the nature of the call before it reaches the U.S. gateway?* Yes, some do. Part of the reason foreign aggregators exist is to obfuscate the real source of the traffic. Given the nature of VoIP and the internet, a foreign robocall originator could trivially send their traffic directly to the US gateway; there is no

technical reason not to do so. They are willing to pay a mark-up imposed by the foreign aggregator to reduce the risk of, and increase the length of time before, being caught. *Are there other mechanisms by which foreign originators of illegal robocalls send their traffic to the United States such that it would be brought onto the U.S. network by an unsuspecting gateway provider?* Foreign originators may set themselves up as US entities so that they do not stand out as foreign. Anybody can get a USA mailing address and phone number, set up a business shell, and rent a server. They can control all that remotely, from anywhere in the world. Still, they must pay some downstream provider(s) to take their calls, and no provider should be “unsuspecting” in this day and age.

31. *We also seek comment on how foreign robocallers and the voice service providers that serve them use U.S. numbers in the caller ID field for their illegal robocall campaigns. Do these entities primarily spoof U.S. numbers?* The primary approach we have observed is random spoofing – they make up a new Caller-ID value for every call or every few calls. In some cases, we have seen them “hijack” numbers that belong to others. But it is trivial for them to alter their methodology; we should not assume that any of this is static. *Or do these bad actors also use U.S. numbers that the voice service provider or their customer has obtained the right to use, either directly from the Numbering Administrator or indirectly through another provider?* Yes, we have also seen this. It is trivial to obtain USA numbers. There are web sites that give them away in small quantities, often for free, and resellers make them available in large quantities for relatively tiny fees. When a number is misused, there are no repercussions; if it is brought to the attention of the sourcing entity, they will likely just disable one number at a time. *We note that the Commission recently proposed rules to help prevent VoIP providers from obtaining numbers directly from the Numbering Administrator for use in illegal robocall campaigns, and there are*

existing reporting rules regarding number usage. Are there other safeguards we should consider to prevent foreign providers from using U.S. NANP numbers in illegal robocall campaigns?

Restricting direct access to number has little impact, because there is such an extensive reseller chain living off those that already have access. Reporting rules are not relevant here, as nobody is required to report “How many of your numbers have been used for illegal calling?” (for example) and it is not clear that any action is or would be taken based on such reports. Note that illegal calling is a rapidly evolving domain, so annual reports that are then subjected to months of pondering are not going to have any impact.

B. Scope of Requirements and Definitions

33. While the Commission has imposed requirements on intermediate providers, including gateway providers, it has never defined “gateway provider” as a distinct category of entities. We now propose to define a “gateway provider” as the first U.S.-based intermediate provider in the call path of a foreign-originated call that transmits the call directly to another intermediate provider or a terminating voice service provider in the United States. In this proposed definition, by “U.S.-based,” we mean that the provider has facilities in the U.S. including a U.S. located point of presence. We seek comment on this proposed definition. Should we define “gateway provider” differently? Should we define “U.S.- based” differently? Should our definition include the first U.S.-based provider in the call path for a foreign-originated call that also terminates that call? While we believe that exploring these details can be helpful in understanding particular calling situations, it would be a mistake to codify this in regulation. As noted, foreign operators can trivially set up a US entity, even with no US-based assets or personnel (and thus nothing to lose in an enforcement action). Should we extend some or all of the requirements we propose today to such terminating voice service providers, or are existing

requirements sufficient? All providers in the call path must bear responsibility for illegal calls. To date, our evidence indicates that terminating providers are rarely close to a source of these calls (because the money they would earn from accepting the calls is trivially small in the scope of their business). *Should we exclude from the definition those providers that serve as a gateway for only a de minimis amount of foreign originated traffic?* All providers must be responsible. Enforcement efforts should be prioritized based on call volume and recidivism, with commensurate penalties. *Are such providers unlikely to be the source of illegal robocalls?* They are unlikely to be the source of a significant number of illegal foreign-sourced calls (an obviously conclusion if they only handle a small amount of foreign traffic, even if ALL of that traffic were illegal). Robocalling, by its nature, is high-volume. *If so, how should we define de minimis for this purpose? Is there another way to effectively limit our definition to apply only to those gateway providers that are especially likely to be the source of illegal calls on the U.S. network?* We do not advocate a volume-based exclusion; it will only be gamed. *Does our definition need to be modified to take into account the scenario where a call originates in the U.S., is routed internationally (over the same provider or a different provider's facilities), and then is routed back to a U.S. end-user through a gateway provider? What about a scenario where a call enters the U.S. through a gateway provider, is routed outside of the U.S. and then back into the U.S. through the same or different gateway provider?* It is increasingly difficult to discriminate between US-based and non-US-based providers. It is important to understand that convoluted routing scenarios exist, but regulations should avoid making these distinctions.

34. *We seek comment on whether U.S.-based providers that fall under our proposed definition of gateway provider also, in some instances, originate calls from abroad carrying U.S. NANP numbers that are brought into the U.S. by that same provider. In other words, are there*

instances where the provider that brings the call into the U.S. is also acting as an originating provider? Absolutely. As BICS points out, many providers choose to know very little about their customers. It is easy to ask a new prospect, “You are a telecom provider, aren’t you?” and be satisfied with a “Yes, I guess so” even if they suspect the prospect is really an end-user call-center or outright fraudster. For such calls, the U.S.-based provider would not fall under our proposed gateway provider definition where it is not acting as an intermediate provider. That is precisely why you should not make such distinctions. Are certain arrangements that are not covered by our proposed definition likely to be part of an illegal robocall campaign? Yes. If so, should we broaden or otherwise modify our proposed definition to ensure that such calls fall within the scope of the protections we propose in this Further Notice? Yes. You should not draw lines; you should not distinguish between foreign or domestic, between intermediate or originating or, for that matter, terminating. Alternatively, should we explicitly include these situations for the purposes of specific rules, such as our proposed mandatory blocking rules? Simpler is better.

35. As we have elsewhere in our caller ID authentication rules, we propose to classify providers as gateway providers on a call-by-call basis rather than on a class basis. Thus, a provider would be a “gateway provider”—and subject to rules applied to that class of provider—only for those calls for which it acts as a gateway provider; it would be an “intermediate provider” or “voice service provider”—and subject to rules applied to those classes of provider—for all other calls, e.g., for domestic-originated calls that it carries. We believe it is appropriate to apply that approach here not only for regulatory symmetry, but also because it would capture all instances in which an entity acts as a gateway provider. At the same time, this approach would not subject all traffic handled by an entity to enhanced obligations

simply because a portion of that traffic originates abroad. We seek comment on this proposal.

All these distinctions (foreign/domestic, gateway/intermediate/voice-service provider) are way too granular. Again, as BICS articulated, providers themselves often do not know. *Should we instead diverge from our “call-by-call” approach for gateway providers?* It is important to understand that the role can vary on a call-by-call basis, but the regulations should not be dependent on this. *Do providers have the ability to treat foreign-originated calls differently on a call-by-call basis?* No, not if they profess as little knowledge about their customers and traffic as BICS indicates. Remember that the objectives of the call launderers are best met if these details are obfuscated and they can deflect the regulations. *If we were to establish that a provider is a gateway provider for all of its traffic, if any traffic it transits originates abroad, would such an approach place unreasonable obligations on a provider’s domestic traffic simply because some traffic is foreign-originated?* It is best if provider obligations not rest on this distinction.

36. *We further propose to limit the scope of our proposed requirements for gateway providers to those calls that are carrying a U.S. number in the caller ID field. By a “U.S. number,” we are referring to NANP resources that pertain to the United States. Under this approach, we would exclude from the scope of our rule those calls that carry a U.S. number in the ANI field but display a foreign number in the caller ID field. We believe that this approach is consistent with our goal to prevent illegal spoofing, which is dependent upon manipulating the caller ID field that is visible to the call recipient. We further propose to apply this requirement on a “call-by-call” basis. Under this approach, a gateway provider would be subject to these requirements for those calls it transits that carry a U.S. number in the caller ID field, but that same gateway provider would not be subject to these requirements for calls displaying numbers associated with another country. We seek comment on these proposals. We also seek comment on*

the feasibility and desirability of widening the scope of our proposed rules to cover calls carrying non-U.S. numbers in the caller ID field or a subset of non-U.S. numbers. If we include a subset of non-U.S. numbers, what numbers should we include? At present, almost all illegal robocalls carry US caller-ID values, so that is the appropriate focus – for now. We must anticipate that as we become more proficient in preventing such calls from entering our network, robocallers will shift to using non-US numbers. First they will use non-US NANP numbers (Canadian and Caribbean area codes, for example); then maybe they will try Australia (a +612 Sydney number is similar to a +1612 Minneapolis number). In fact, while authoring this document, I received a fraud robocall (Amazon impersonation) claiming to be from a +33 number (France); I know the number to be invalid because it has the wrong number of digits for the French dialing plan. Regardless of the caller-ID value, providers should be looking for high-volume, short-duration traffic flows and permitting them only on an exception basis, when they know with certainty that the calls are legitimate. Your rules should do no more than anticipate such maneuvers (and thus not be specific to any particular caller-ID values).

37. Limiting our proposed rules to calls that use U.S. numbers in the caller ID field is similar to the approach in our current rule that requires intermediate providers and voice service providers to not accept calls directly from a foreign voice service provider that is carrying U.S. numbers if the foreign voice service provider is not listed in the Robocall Mitigation Database. In that context, we limited application of our rule to foreign voice service providers that “use[] North American Numbering Plan resources that pertain to the United States.” We seek comment on whether it is appropriate, in this context, to take a narrower or more expansive approach than we did in the context of foreign voice service providers whose traffic must be blocked if they are not listed in the Robocall Mitigation Database. The existing

rule was a good starting point that obviously triggered much thought and discussion. Ultimately, however, no entity, in any country (including our own), using any caller-ID values (including foreign), is entitled to bombard our residents with illegal calls. It would make no sense to have a rule that, effectively, says “Foreign-based illegal robocallers, and all of their downstream co-conspirators (be they foreign or domestic), are absolved of culpability if the caller-IDs of the calls pertain to numbers outside the NANP.”

C. Authentication

40. *We propose concluding that, given the key role gateway providers play in allowing foreign calls into the United States, gateway providers should be required to authenticate unauthenticated foreign-originated SIP calls that they receive and cooperate with traceback requests with respect to those same calls. Requiring gateway providers to authenticate caller ID information for all unauthenticated foreign-originated SIP calls will offer information to the downstream providers regarding where a foreign-originated robocall entered the call path, facilitating analytics and promoting traceback efforts. We seek comment on this proposal.* To the extent that Call Authentication is helpful, it should be required of ALL providers prior to the terminating provider. As noted earlier, authentication in and of itself does not deter illegal robocalling; it has to be more ubiquitous, and the authentication information has to be incorporated systemically into scaled mitigation practices.

41. *Even with a “C-level” (gateway) attestation, we anticipate that authenticating unauthenticated calls will facilitate faster traceback and improve call analytics. We seek comment on this analysis and on the possible benefits of the requirement we propose.* Traceback is already very fast in most cases (hours to a day or two) compared to other elements of the robocall mitigation process (time for the sourcing provider to investigate and respond; time for

any enforcement action to be initiated and concluded). Unless and until those elements are sped up, shaving a few hours off traceback via call authentication will not be meaningful. Analytics could indeed be improved with authentication data, provided that the fraction of authenticated calls grows substantially, and that authentication gaming (such as noted above, where downstream providers authenticate on behalf of their upstreams, without identifying the actual source) is caused to cease. We observe, for example, many calls authenticated (with C-level attestation) by Lumen. Lumen is a huge intermediate provider (as well as an originating provider) with perhaps thousands of customers. While it is notable that Lumen is trying to be helpful, providing authentication where their upstreams have not, that authentication, in and of itself, reveals nothing.

D. Robocall Mitigation

53. We seek comment on this proposal [regarding traceback]. Is a mandatory 24-hour response time appropriate, or should we consider a different response time? Our experience implementing and operating the original traceback portal suggests that response time generally is not a significant issue. Most providers had one or more individuals assigned to respond to traceback requests, and during normal business hours, many responded in minutes. From its inception, the traceback portal has tracked response time and made each provider aware of their track record. At the first in-person meeting of providers after deployment of the portal, we handed out awards to those providers that were the quickest. Because gateway providers are already required to respond to traceback “timely,” we believe that this enhanced requirement presents a minimal burden on gateway providers. We seek comment on this tentative conclusion. Are there any instances where a gateway provider may need more time to respond? If so, what would cause such a delay (e.g., what are the technical and/or operational challenges that would

contribute to the delay)? How might we address any such problems to best enable gateway providers to meet such a requirement? The Fourth Report and Order already indicates “We generally expect responses within a few hours, and certainly in less than 24 hours absent extenuating circumstances. Patterns of delayed response may lead to Commission enforcement.”¹⁹ This guidance has proven sufficient for providers that want to be part of the solution. Providers that are part of the problem will ignore and evade the rules. *Should we instead consider requiring response in a shorter time than 24 hours? Are there additional benefits or burdens to requiring a faster response time? Are there any other issues we should consider in adopting such a requirement, such as the impact on small gateway providers?* We do not believe differentiated response times for gateway providers are necessary or particularly useful. The Designated Consortium should continue to track response times; lagging providers should be considered non-responsive based on the Consortium’s evaluation. For some providers (for example, the major wireless providers, one of which is involved in almost every traceback), there could be an occasional request that slips through the cracks; it does not seem appropriate that they be penalized if in the vast majority of cases they are responding very quickly. And for all this discussion of response time requirements, there is no mention of what happens when that mandate is not met. A regulation with no teeth will not be meaningful.

54. *We seek comment on other means to improve traceback when calls originate internationally. Are there other, or additional, steps the Commission could take to improve this process and make bad actors easier to identify and stop?* Downstream providers are in the best position to gain traceback cooperation from their upstreams. Downstreams should quickly be made aware (automatically, via the traceback process) when an upstream is slow responding or

¹⁹ Fourth Report and Order at footnote 52; referenced at FNPRM footnote 137.

fails to respond to a traceback request. More generally, a major impediment to traceback effectiveness is the secrecy that surrounds the findings. We know that problematic providers (be they foreign or domestic) often have multiple paths into the network, and work constantly to acquire new ones. The provider community should be made aware of which providers are currently facilitating illegal calls so that they can be proactive in screening traffic and prospects. *Should the Commission consider taking these steps in addition to, or instead of, requiring gateway providers to respond within 24 hours?* While we have identified that many problematic calls originate internationally, the associated tracebacks do not warrant special attention. To the extent that outreach to foreign regulators (see FNPRM para. 52) is going to result in some rapid (hours or days) response is pure folly, in our experience. US enforcement organizations do not act that quickly when the problem is right here at home. Improving traceback transparency is a simple non-technical enhancement that can be implemented immediately. *What benefit would these approaches provide?* Commercial operators can act very swiftly, turning off a problematic upstream in a matter of hours if not minutes if they are motivated to do so. That will deliver a greater reduction in time-to-mitigate than any reduction in the time spent on actual traceback, which is already quite low. *Are there any particular burdens or concerns the Commission should consider when weighing these options?* The Commission should ensure that identified providers have the opportunity to rebut or explain traceback findings; this could be as simple as allowing those providers to post their own statements on a website created for this information-sharing purpose. To the extent that the designated consortium is unable or unwilling to proactively share time-critical traceback details, the Commission should routinely obtain that information from them and post it for everyone's benefit.

57. Specifically, we propose to require gateway providers, following a prompt investigation to determine whether the traffic identified in the Enforcement Bureau's notice is illegal, to promptly block all traffic associated with the traffic pattern identified in that notice. We seek comment on this proposal. We wholeheartedly support this approach. However, the notion of "traffic pattern" is problematic. We believe the sourcing provider should be removed from the RMD (if present) and ALL providers should reject ALL calls from that source. This approach should apply regardless of whether the notified provider is acting as an intermediate provider or an originating provider, and regardless of whether the source claims to be a provider itself, or is a call originator.

58. We seek comment on whether allowing gateway providers to investigate prior to blocking strikes the correct balance. Providers routinely complain that they do not want prescriptive regulations. Different levels of urgency and corrective action may be indicated depending on the severity of the problem. When the Commission notifies a provider about a problem, that provider is in the best position to assess the situation. One approach would be to make the notified provider liable for any calls from that source that it passes subsequent to the notification; perhaps at a rate of \$100 per any illegal call. That would motivate the provider to quickly investigate, and to consider, based on their history with the traffic source and their knowledge of their call history, whether an immediate full suspension was warranted during the investigation. A prudent provider would establish, in advance, that it could recover any fines from the source, and might demand a bond or other prepayment before accepting traffic from certain prospective (unknown) sources. Remember that in this business, it is all about the money.

59. We seek comment on the contours of the blocking obligation. Should we require the notified gateway provider to block all calls that meet criteria identified by the Enforcement

Bureau in its notice that make it highly likely that the calls are part of the same call pattern as those calls that the Commission has determined to be illegal? We reiterate our note above that “call pattern” is problematic, even if you attempt to better define it. An economic liability leaves the detailed evaluation up to the notified provider, who has the best available information.

60. In conjunction with our mandatory blocking proposal above, we propose that, should a gateway provider fail to comply with those requirements, the Commission, through its Enforcement Bureau, may send a notice to all providers immediately downstream from the gateway provider in the call path. Upon receipt of such notice, all providers must promptly block all traffic from the identified gateway provider, with the exception of 911 and PSAP calls. We seek comment on this approach. Again, we support something along these lines. We believe that this overlaps the already-present approach (yet to be exercised) of deleting the gateway provider from the RMD.

61. [W]e believe there is value in requiring the voice service provider or intermediate provider immediately downstream from a gateway provider to block all calls from that gateway provider in the event that the gateway provider fails to effectively mitigate, or block if required, illegal traffic once notified of such traffic by the Commission via the Enforcement Bureau. We seek comment on this view. This is the correct view.

62. We seek comment on how much time gateway providers should have to begin effectively mitigating, or blocking, calls before directing downstream providers to block all calls from that gateway provider. We are unclear whether this delay includes or excludes the time to “investigate,” which was discussed earlier. Rejection of traffic should occur immediately once there is a determination or notification regarding a particular source. Technically, this can

happen very quickly – in minutes at most. Providers are very adept at blocking traffic when, for example, a pre-paid balance is depleted. This should happen at least that fast.

63. We seek comment on how much time to permit downstream providers to begin blocking calls from the identified gateway provider. See 62.

64. We seek comment on how much time to permit downstream providers to begin blocking calls from the identified gateway provider. ... Is there some other approach that would be more appropriate, such as a public notice or use of the Robocall Mitigation Database? We also seek comment on how we can determine whether a downstream provider is complying with this blocking requirement. Should we require the downstream provider to block all calls from the identified gateway provider, or just those that are part of the identified call pattern? This is an perfect use of the RMD. Providers can sign up to receive notifications about RMD changes. The problematic provider should be delisted, triggering a notification to all providers. We would note that “delisting” should not actually constitute complete removal from the database; rather, an entry should be retained so that it is clear to all others that the problematic provider has been explicitly designated as such. This will ensure that if (when) the problematic provider attempts to shift their traffic to a new downstream, that downstream will become aware of the situation before enabling the traffic. The requirement (consistent with current RMD rules) should apply to ALL traffic; we reiterate our opposition to reliance on “call patterns.”

65. Finally, we recognize that blocking of all traffic from a particular gateway provider is likely to have a profound impact on that gateway provider’s ability to do business. We therefore seek comment on whether to adopt additional due process steps or requirements to ensure that these rules are not erroneously applied to gateway providers. Is allowing investigation prior to requiring blocking sufficient, or should we adopt additional protections?

As we noted earlier, eradication of illegal robocalls is going to force some providers to find another line of work. Providers already have ample opportunity to rid their networks of problematic calls in an orderly fashion. By the time they hear from the FCC, their own monitoring tools, if they have any, have failed, and they have probably already been the subject of multiple traceback requests. That, along with an investigation opportunity, is plenty of due process.

66. Specifically, we propose to require gateway providers to: 1) incorporate caller ID authentication information where available; 2) manage the blocking with human oversight and network monitoring sufficient to ensure that it blocks only calls that are highly likely to be illegal, which must include a process that reasonably determines that the particular call pattern is highly likely to be illegal before initiating blocking of calls that are part of that pattern; 3) cease blocking calls that are part of the call pattern as soon as the gateway provider has actual knowledge that the blocked calls are likely lawful; and, 4) apply all analytics in a non-discriminatory, competitively neutral manner. We seek comment on these proposals. We believe that these proposals, while sound advice, are too granular for regulations. The onus must be on providers to do whatever is necessary to block mass illegal calling campaigns, and to employ methods to discriminate between legal and illegal campaigns to avoid improper blocking. Recall that these calls are virtually all exchanged via commercial agreements and providers accepting traffic on that basis do not need FCC permission to reject potentially problematic traffic, nor should the FCC attempt to mandate them to accept traffic that the provider determines is potentially risky. These comments apply to FNPRM paragraphs 67-70 as well.

81. We propose and seek comment on requiring gateway providers to confirm that a foreign originator is authorized to use the particular U.S. number that purports to originate the

call. We further propose to make clear that this requirement applies only when an originator seeks to place a high volume of calls using a U.S. number, and does not apply to traffic consistent with private, individual use. The requirement should apply to ALL high-volume traffic, not just that from foreign sources, and not just that flowing through gateway providers.

82. *We seek comment on how a gateway provider can best comply with this requirement. Is it feasible for a gateway provider to obtain useful information?* All high-volume traffic, whether foreign-sourced or domestic, should be treated as radioactive. This traffic, which the industry generally also refers to as call center, CC, dialer, short-duration, high-velocity, or non-conversational, should not be accepted via aggregators (foreign or otherwise). It should flow directly to a (US-based) provider equipped to validate and monitor the traffic. That provider should verify the validity of the calling campaigns and place appropriate restrictions on the caller-ID values allowed. Providers not in a position to successfully take on this burden must not accept this kind of traffic.

83. *We seek comment on the scope and extent of this requirement. Should we adopt a carve out to ensure that gateway providers do not prevent origination of emergency calls, including calls to 911, calls from PSAPs, or calls from government emergency outbound numbers?* We would expect the vast majority of 911 calls to flow via trunks dedicated to that purpose. Emergency calls that are translated to 10-digit NANP numbers would be part of conversational traffic flows, NOT high-volume flows. OUTBOUND traffic from government emergency agencies (e.g., “reverse 911” calls) should be handled like any other high-volume traffic – sent via providers that are suitably equipped. *If so, what might this look like? In addition, we specifically propose to impose this requirement only where the originator seeks to place a high volume of calls. We seek comment on this proposal.* Indeed, high-volume calling

deserves the highest level of scrutiny. *We are concerned about ensuring that individual callers, such as U.S. residents traveling abroad, are not prevented from placing calls using a number to which they are subscribed while in a foreign country.* Roamer traffic should flow via conversational trunks, segregated from high-volume traffic. See additional roaming comments below. *To address this, should the requirement only be triggered after the gateway provider sees a set number of calls purporting to originate from a particular U.S. number? If so, what is the appropriate threshold to constitute a “high volume” of calls?* Your rules in this context most definitely should not be dependent on counting calls from particular US numbers. Legitimate high-volume traffic should come from a few pre-designated numbers. Conversational traffic has a different distribution of call durations and may come from few or many different numbers.

With respect to US residents traveling abroad: this has been discussed extensively in this docket, first triggered by comments filed by USTelecom in response to the DRAFT NPRM²⁰, and subsequently by a petition filed by CTIA.²¹ CTIA writes:

Call completion is a primary objective and consumer expectation in our connected, global telecommunications system, and is made possible for U.S. consumers when travelling or living abroad through international wireless roaming, including 3G wireless roaming. Wireless roaming is a complex endeavor, which is more complicated internationally, as U.S. mobile network operators have roaming agreements with hundreds of overseas network operators to enable U.S. consumers to remain connected no matter where they travel or move. There are over 750 global mobile network operators, and there is at least one foreign provider in each country that interconnects with U.S. providers. *When a mobile wireless consumer abroad uses a U.S. phone number to call a consumer in the United States, that call may be routed from an originating foreign provider’s network over long distance routes that involve multiple foreign mobile network operators often on the basis of least cost routing to reach a U.S. intermediate or terminating provider for delivery to the intended recipient. Under this framework, there are a number of hand-offs*

²⁰ USTelecom Notice of Ex Parte, Sep. 18, 2020, see “roaming” references on pages 2 and 5
<https://ecfsapi.fcc.gov/file/109181882106534/USTelecom%20Ex%20Parte%20Notice%20on%20Draft%20Second%20Report%20and%20Order%20-%20FINAL.pdf>

²¹ CTIA Petition for Partial Reconsideration, Dec. 17, 2020
<https://ecfsapi.fcc.gov/file/1217260238820/201217%20CTIA%20Petition%20for%20Partial%20Reconsideration%20-%20FINAL.pdf>

*for a call on its way back to a U.S. consumer, and any one of hundreds of foreign providers could be chosen as the final foreign provider in the call path that interconnects with a U.S. intermediate or terminating provider.*²²

We hark back to earlier action before and by the Commission related to Rural Call Completion. There, we learned that multiple call hand-offs driven by least cost routing are a recipe for disaster when it comes to completing calls. When an incentive was imposed limiting calls to two intermediate hops, the rural call completion problem was largely eradicated.

CTIA expressed concern that pending rules posed “a substantial risk that U.S. citizens traveling or living abroad, as well as military and diplomatic personnel that are often deployed to remote and dangerous regions of the world, cannot complete calls back to the United States.”²³ CTIA members should be even more concerned about haphazard routing by their partners of those calls over uncertain (and likely insecure) pathways that could include grey routes and fraud.

We understand that these calls are precious, not only to the calling and called parties, but to the providers. The major US wireless providers publish retail rates for casual international roaming that range up to \$3 per minute. Yet wholesale rates to the USA are some of the cheapest on the planet – typically under a penny per minute. When call completion is the priority, risking that via least-cost routing would appear to be a poor choice.

Getting legitimate foreign-originated calls safely, securely and reliably into the United States is best achieved by having those calls routed from the source DIRECTLY to a responsible US-based provider equipped to manage the traffic. Use of foreign intermediaries and aggregators of indeterminate reputation must be avoided. Happily, if they did not know it before, the industry

²² CTIA, page 3, footnotes omitted, emphasis added

²³ CTIA, page 6

put itself on notice in September of last year when USTelecom made its filing. They have had almost 15 months to implement any required fixes. If they have not done so, then the calls must not be as precious as previously claimed.

84. *Upstream Provider as the “Customer.”* Alternatively, should we impose a requirement similar to the rule adopted in the Fourth Call Blocking Order, and require gateway providers to take steps to know the upstream providers from which they receive traffic and prevent those providers from originating illegal traffic onto the U.S. network? All providers should take effective measures to prevent illegal traffic from moving via their platforms. It does not matter if they know their customer or not. It matters little if the traffic is “originating” on that provider’s network or not.

85. *Alternatively, should we consider the call originator the gateway provider’s “customer” for purposes of such a requirement?* We believe that the originator, as the entity placing the calls, is probably the most relevant “customer” for the purpose of stopping illegal calls. Unfortunately, the gateway provider, in many cases, may have no direct relationship with the originator, making it significantly more difficult to obtain information. We seek comment on considering the call originator the “customer” for purposes of a know-your-customer requirement. What would be sufficient for a gateway provider to reasonably claim that it “knows” this “customer”? These questions demonstrate how impossible it will be for providers and enforcers to know whether rules are or are not being violated. High-volume traffic should come directly to US-based providers that are equipped to vet and police it. This traffic should not be permitted to be obfuscated by intermediaries that then feign ignorance. To the extent that aggregators (be they foreign or domestic) need to exist, they should carry conversational traffic exclusively.

88. *We seek comment on what specific contractual provisions, if any, we should require. Should we require gateway providers to ensure by contract that their foreign partners validate that the calling party is authorized to use the U.S. NANP telephone numbers, for calls with such numbers in the caller ID display? Are we correct in anticipating that if a foreign partner cannot validate the number, there is a significant risk that the number is being spoofed and is therefore likely to be involved in an illegal robocalling campaign? How should we address circumstances in which the foreign partner cannot validate the number on its own? For instance, should we require the gateway provider to require foreign partners by contract to use a third-party telephone number validation service?* All your questions beget more questions. It is up to each provider to decide what to put in their contracts, and how they enforce those provisions. The Commission should require simply that the provider take effective measures to prevent their platform from being used to transmit illegal robocalls. The provider must take responsibility for how that is done. The industry may come up with best practices to be shared, if individual providers cannot figure it out for themselves. To the extent that any given provider struggles to find an effective methodology, their safe harbor is to exit the business.

89. *We seek comment on implementation of any requirement to adopt specific contractual provisions.* The FCC is not equipped to give this advice. Leave this to private legal counsel.

91. *In addition to the specific mitigation requirements for which we seek comment above, we also propose to require gateway providers to meet a general obligation to mitigate illegal robocalls. Robocallers have shown that they can adapt to specific safeguards targeting illegal traffic. A general obligation can serve as an effective backstop to ensure that robocallers cannot evade any granular requirements we adopt.* Precisely. Proposed granular requirements will be subject to evasion and dispute. Put your energy into general obligations which you will then

enforce. ... *The Commission stated that a program is “insufficient if a provider knowingly or through negligence serves as the originator for unlawful robocall campaigns.” We believe imposing an analogous requirement on gateway providers would provide a valuable backstop and help reduce the likelihood that illegal robocalls might make their way to U.S. consumers. Under this approach, gateway providers would be required to take reasonable steps to avoid transiting illegal robocall traffic.* This requirement should be imposed on ALL providers. *What would be the benefits and drawbacks of doing so? What would constitute “reasonable steps” in this context, aside from any of the actions proposed in this Further Notice? Would the consistency of obligations between gateway providers and voice service providers facilitate innovation and development of novel, effective robocall mitigation techniques?* A variety of techniques have and will be proposed, here and, for example, in settlement agreements reached by State Attorneys General. They are not necessarily novel; in fact, some are obvious. They will be continuously evolved so that they remain effective.

92. *Should we require gateway providers to take affirmative, effective measures to prevent current, new, and renewing customers from using their network to transit illegal calls? Are other modifications appropriate? Replace “current, new, and renewing” with “all.” Simpler is better. (With your proposed language, some idiot will claim that their “former” customer is outside the scope.) Require this of ALL providers, not just gateways. *Instead or in addition to making such modifications, should we provide additional guidance to gateway providers about what measures would be deemed “affirmative” and “effective”? What should that guidance be?* Affirmative and effective are good words. Affirmative means you do it without being explicitly instructed to do so in a reactionary way. Effective means it works. Traceback means you flunk.*

E. Robocall Mitigation Database

96. *We propose requiring gateway providers to submit the same information that voice service providers must submit under Commission rules.* We believe the public interest will best be served if ALL providers are required to register in the RMD, regardless of their role(s). For each provider, there should be a statement regarding their STIR/SHAKEN implementation status, and also, in all cases, a Robocall Mitigation Plan subject to at most minimal redaction. There should be contact information. It seems unlikely that the FCC will audit or enforce proactively the veracity of this content. If a provider's behavior is found to be inconsistent with their registration and certification, penalties should be swift and severe. Delisting is a good start.

97. *Similar to our recently proposed rules for VoIP direct access applicants, should we require gateway providers to “inform the Commission” through an update to the Robocall Mitigation Database filing, if the gateway provider is “subject . . . to a Commission, law enforcement, or regulatory agency action, investigation, or inquiry due to its robocall mitigation plan being deemed insufficient or problematic, or due to suspected unlawful robocalling or spoofing . . . ”?* We are doubtful that misbehaving providers will comply with such a rule.

98. *We propose to extend the prohibition on accepting traffic from unlisted providers to gateway providers.* We believe that all providers should be prohibited from accepting traffic from another provider not listed in the RMD, regardless of the roles of the various providers (which have been shown to be difficult to definitively discern); gateway providers should not be differentiated. There should be only one entry per provider (not multiple, as we see today for providers that act as both originating and intermediate providers). But it must be recognized that an (originating) provider can routinely claim that the call source is their “customer” (in other words, that they are originating the call on behalf of a non-provider source). As noted earlier,

providers that are “de-listed” should be noted as such in the RMD, and providers would then be prohibited from accepting traffic from a de-listed entity whether that entity was claiming to be a provider or otherwise. For a legitimate, reputable provider, the advantage of traffic from a listed provider could be that the FCC would discount (but not eliminate) associated penalties against the downstream if the traffic was found to be illegal.

100. *We take this opportunity to seek comment on whether we should require Robocall Mitigation Database filers—including voice service providers and, if required, gateway providers—to submit additional identifying indicia, such as a Carrier Identification Code, Operating Company Number, and/or Access Customer Name Abbreviation. We anticipate that requiring some additional identifying information may ease compliance by facilitating searches within the Robocall Mitigation Database and cross-checking information within the Robocall Mitigation Database against other sources. Do commenters agree?* More information could be helpful, but making this information mandatory is problematic. Many providers do not have a CIC or OCN or ACNA. Many DO have a 499A Filer ID; this would be good to have when it exists. Providers go by many names and mergers are routine, making it hard to know definitively which entry applies to whom when names overlap. Today, the “unique ID” in the database is the FRN; even there, there are overlaps. (It would be helpful if the RMD “Other FRNs” field were in a standardized format. It might also be helpful if providers could list a Parent or Master FRN; see for example all the subsidiaries in the RMD associated with Verizon or with Lumen.) Once again, however, we note that the bad guys just apply, and get, new FRNs or 499A Filer IDs since these are not vetted in any way. Soliciting information is only helpful if that information is valid, and is likely to be valid only if there are consequences for it being invalid. We believe that the Contact Email address and the Contact Telephone Number are useful and critical pieces of data.

If they are found to be non-functional (for example, in the course of an FCC formal investigation or informal inquiry), then the provider should expect to be de-listed the second business day after notice is served via overnight delivery to their Contact Business Address. That will encourage them to get these data items correct and to monitor messages they are sent. (Incidentally, in the course of our work, we found at least one Contact Email that yielded “Bad destination mailbox address.”)

101. *We take this opportunity to clarify that even if a voice service provider (or, if we adopt our proposal in today’s Further Notice, a gateway provider) is not listed in the Robocall Mitigation Database, other voice service providers and intermediate providers in the call path must make all reasonable efforts to avoid blocking calls from PSAPs and government outbound emergency numbers.* We will go on the record stating that this requirement is impractical, unhelpful and not particularly relevant, depending on the interpretation of “in the call path” and “all reasonable efforts.” Example: Providers routinely open their network firewalls only to customers with whom they have active relationships. This is a standard best practice to prevent hacking and denial-of-service attacks. If Provider X is de-listed and thus other providers end their relationships with X, it would be unreasonable for those downstream providers to keep their firewalls open to X. Furthermore, if Provider X then decided to send calls to other providers with whom it had never had a prior relationship, it would not be reasonable to expect those other providers to accept calls from X even if they were from PSAP/government emergency numbers. And maintaining a list of all such numbers to ensure compliance with this contemplated rule would be a nightmare in and of itself and would be a target for abuse.

102. See responses to 101 and also 83.

F. Alternative Approaches

104. *We first seek comment on strengthening our prohibition on U.S.-based providers accepting traffic carrying U.S. NANP numbers that is received “directly from” foreign voice service providers that are not in the Robocall Mitigation Database. By its terms, this rule does not require U.S.- based providers to reject foreign-originated traffic carrying U.S. NANP numbers that is received by a U.S. provider directly from a foreign intermediate provider—at present, the prohibition only applies to traffic received directly from the originating foreign provider.* This is an unfortunate interpretation of the rule. Our general preference is to read the rules in ways that discourage illegal robocalling rather than the opposite. In this case, we would interpret “directly from” to mean “not through some other US-based provider.” And as we have noted elsewhere, it is difficult if not impossible to know when a provider is acting as a “voice service provider” versus an “intermediate provider.” The safe bet is to treat all foreign providers as voice service providers. The phraseology could be simplified to eliminate any of these uncertainties. More generally, even domestically, this distinction should be eliminated.

105. *Conversely, should we limit or eliminate the foreign provider prohibition rather than expand it?* We pointed out, in the context of the CTIA motion, that US-based providers, rather than fretting over foreign providers, could act as the ORIGINATOR of the calls they received, and take responsibility for them. To the extent that a commenting provider thinks that placing constraints on foreign providers is burdensome or poses jurisdictional issues or might result in diplomatic repercussions, this alternate avenue is available. In fact, our own preference is that the burden for keeping illegal robocalls off our network should fall ENTIRELY on US-based providers because we think timely enforcement, which must be part-and-parcel of any rulemaking, is largely hopeless against foreign entities.

G. Expected Benefits and Costs

109. *We anticipate that the impact of our proposals, including the deterrence that arises from authenticating unauthenticated foreign-originated calls, will account for a large share of that \$13.5 billion benefit because of the significant share of illegal calls originating outside our country. While each of the proposed requirements on their own may not fully accomplish that goal, viewed collectively, we expect that they will achieve a large share of the \$13.5 billion minimum benefit. We seek comment on this analysis and on the possible benefits of the requirements we propose.* We agree that significant benefits can come from the outcome of this proceeding providing that it is timely enforced. We also believe that significant benefits would come from broad and timely enforcement of rules already in place. We disagree with the emphasis on “authenticating unauthenticated foreign-originated calls.” Authentication is not, in and of itself, particularly helpful near-term. New rules that augment authentication (such as Robocall Mitigation Programs and requirements that providers take affirmative and effective action) are more likely to produce the desired results (with appropriate enforcement).

110. *We believe that the costs imposed on gateway providers by our proposed changes, at least some of which are likely minimal, will be far exceeded by the expected benefits. Moreover, as the Commission stated in the First Caller ID Authentication Report and Order and Further Notice of Proposed Rulemaking, an overall reduction in illegal robocalls will greatly lower providers’ network costs by eliminating both the unwanted traffic congestion and the labor costs of handling numerous customer complaints.* We agree with this analysis. We note (again) that the biggest “cost” associated with successful mitigation of illegal robocalls will be the loss of tens of millions of dollars that the fraudsters pay annually to the cottage industry that facilitates their calls. Gateway providers that depend largely on illegal calls will go out of business.

111. *[W]e seek comment on how our proposals may promote or inhibit advances in diversity, equity, inclusion, and accessibility, as well the scope of the Commission's relevant legal authority.* The FCC has attributed \$3.5 billion of annual illegal robocall economic cost to the 10 cent per call annoyance factor, and a much larger amount, \$10.5 billion, to fraud losses. Those fraud losses are often borne by the more vulnerable in our population – those that may speak English as a second language, or be economically disadvantaged, or have some other emotional, physical, or social challenge. These individuals are the ones most harmed by illegal robocalls and are most deserving of rules, efforts and investments that will minimize future damage.

SUMMARY AND CONCLUSIONS

We believe the existing rules should be evolved along these lines:

- All providers must be part of the solution to the illegal robocall mitigation challenge. Rules should apply regardless of whether a provider plays an originating or intermediate role (since they are difficult to distinguish and change call-by-call).
- Recognize that illegal robocalls travel as high-volume traffic flows. This traffic must be subject to greater scrutiny than conventional conversational traffic.
- The rules should be as objective as possible and must acknowledge that problematic providers will attempt to game whatever system we put in place.
- Burdens on those placing and transiting conversational traffic should be minimized.

In the table below, we propose an approach that reflects the issues raised in the FNPRM and incorporates what we know from extensive involvement with parties in all corners of the ecosystem.

Rule / Consideration	Explanation / Rationale
Traffic must be segregated into Conversational and Non-Conversational Flows (CF and NCF). A provider that accepts an NCF must abide by the stipulations below. A flow that meets the criteria for conversational traffic is not subject to constraints placed on NCFs.	Illegal robocalls are initiated as NCFs; that is the best place to detect and mitigate them. Attributes of an NCF are difficult to game. Alternatives (KYC, database filings, contract stipulations, foreign vs. domestic distinctions, etc.) are ripe for deception, which is the illegal callers' stock-in-trade.
A traffic flow is a collection of calls that a provider receives from a single source. The most relevant parameters for each call are the called and calling numbers, the start date and time, and the call duration.	Flows can be readily evaluated at either end (by the source and by the receiving provider). Both parties have access to identical data.
Conversational traffic is traffic that meets metrics associated with conventional human-to-human calling. A CF will have average call duration of at least 120 seconds AND at least 20% of the calls will last longer than 2 minutes.	The listed values are relaxed from what is observed on mobile networks (where virtually all calls are human-initiated), and thus provide a rational starting point, which can be adjusted with additional data and experience.
Providers must ensure that all CFs meet the specified metrics.	Each provider decides whether to use network constraints, on-going monitoring, periodic auditing, contractual provisions (perhaps with indemnification), or other means.
A provider opting to accept NCFs must constrain and monitor each flow to the extent necessary to ensure that it does not contain detectable illegal calls.	It is up to the provider to determine the appropriate measures. Best practices include vetting and constraining the caller-ID values that are permitted and monitoring those values for illegal calling (via, for example, analytics, voice-mail captures, and DNC complaints).
All calls in an NCF must be authenticated, meaning that a provider that accepts a non-authenticated call in an NCF must authenticate it before sending it onward. This includes a requirement to re-authenticate calls received over legacy links.	To the extent that STIR/SHAKEN can be helpful, its deployment should be mandated on NCFs, where the majority of illegal robocalls lurk. CFs are unlikely to contain a substantial number of illegal robocalls.
Enforcement will start with the provider closest to the call source as determined via S/S and/or traceback and will move downstream if a provider is non-responsive. Penalties (including RMD de-listing) will scale according to recidivism and the extent of the non-compliance.	Providers get credit for striving to comply. Enforcement and penalties are focused on the worst abusers. The system rewards stakeholders for segregating NCF and carefully scrutinizing it.
No provider may accept a CF or NCF from an entity that has been de-listed in the RMD.	Alerts all providers to bad actors; creates a barrier to provider shopping.
ALL providers are subject to these rules regardless of their role in the call path.	This avoids vagaries and gaming related to how providers and customers are classified.

The FNPRM attempts to exhaustively explore various regimes for new rules, and rightly recognizes that many illegal calls are perpetrated by overseas fraudsters. But the FNPRM also exposes the challenges of basing rules on any number of differentiating factors. Of all the factors raised in the FNPRM, high-volume calling is most directly correlated to illegal robocalling and where we should focus our efforts. Not only does this maximize the energy expended in the direction where it will do the most good, it also minimizes the burden on most innocent bystanders.

Our approach makes it difficult for aggregators to pollute their traffic streams with illegal calls. Legitimate robocallers will be encouraged to partner directly with scrupulous providers to enable their NCF traffic. These callers must recognize that their biggest enemy is their ILLEGAL counterparts; eliminating (or minimizing) that constituency makes everybody's life easier.

Respectfully submitted,

DATED: 7 December 2021

/s/ David Frankel
dfrankel@zipdx.com
Tel: 800-372-6535